

By: Ellis

S.B. No. 1036

A BILL TO BE ENTITLED

AN ACT

relating to information technology security practices of state agencies.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subchapter F, Chapter 411, Government Code, is amended by adding Section 411.1406 to read as follows:

Sec. 411.1406. ACCESS TO CRIMINAL HISTORY RECORD INFORMATION: DEPARTMENT OF INFORMATION RESOURCES. (a) The Department of Information Resources is entitled to obtain from the department or another appropriate law enforcement agency the criminal history record information maintained by the department or other law enforcement agency that relates to:

(1) a person who is an applicant for employment with the Department of Information Resources;

(2) a person who may perform services for the Department of Information Resources; or

(3) a person who is an employee or subcontractor, or an applicant to be an employee or subcontractor, of a contractor that provides services to the Department of Information Resources.

(b) Criminal history record information obtained by the Department of Information Resources under Subsection (a) may be used only to evaluate:

(1) an applicant for employment with the Department of Information Resources;

1 (2) a person who may perform services for the
2 Department of Information Resources; or

3 (3) a person who is an employee or subcontractor, or an
4 applicant to be an employee or subcontractor, of a contractor that
5 provides services to the Department of Information Resources.

6 (c) Criminal history record information obtained by the
7 Department of Information Resources under this section may not be
8 released or disclosed to any person or agency except on court order
9 or with the consent of the person who is the subject of the
10 information.

11 (d) The Department of Information Resources shall destroy
12 the criminal history record information obtained under this section
13 after the information is used for the purposes authorized by this
14 section.

15 SECTION 2. Subchapter D, Chapter 551, Government Code, is
16 amended by adding Section 551.089 to read as follows:

17 Sec. 551.089. DEPARTMENT OF INFORMATION RESOURCES. This
18 chapter does not require the governing board of the Department of
19 Information Resources to conduct an open meeting to deliberate:

20 (1) security assessments or deployments relating to
21 information resources technology;

22 (2) network security information as described by
23 Section 2059.055(b); or

24 (3) the deployment, or specific occasions for
25 implementation, of security personnel, critical infrastructure, or
26 security devices.

27 SECTION 3. Section 552.139, Government Code, is amended to

1 read as follows:

2 Sec. 552.139. EXCEPTION: GOVERNMENT INFORMATION RELATED TO
3 SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS. (a) Information
4 is excepted from the requirements of Section 552.021 if it is
5 information that relates to computer network security, to
6 restricted information under Section 2059.055, or to the design,
7 operation, or defense of a computer network.

8 (b) The following information is confidential:

9 (1) a computer network vulnerability report; and

10 (2) any other assessment of the extent to which data
11 processing operations, a computer, [~~or~~] a computer program,
12 network, system, or system interface, or software of a governmental
13 body or of a contractor of a governmental body is vulnerable to
14 unauthorized access or harm, including an assessment of the extent
15 to which the governmental body's or contractor's electronically
16 stored information containing sensitive or critical information is
17 vulnerable to alteration, damage, [~~or~~] erasure, or inappropriate
18 use.

19 (c) Notwithstanding the confidential nature of the
20 information described in this section, the information may be
21 disclosed to a bidder if the governmental body determines that
22 providing the information is necessary for the bidder to provide an
23 accurate bid. A disclosure under this subsection is not a voluntary
24 disclosure for purposes of Section 552.007.

25 SECTION 4. Subchapter C, Chapter 2054, Government Code, is
26 amended by adding Sections 2054.064 and 2054.065 to read as
27 follows:

1 Sec. 2054.064. VULNERABILITY STANDARDS. (a) The
2 department by rule shall establish standards for protection of
3 computers, computer programs, computer networks, computer systems,
4 interfaces to computer systems, computer software, and data
5 processing of state agencies and of contractors of state agencies
6 from internal and external unauthorized access or harm, including
7 alteration, damage, theft, erasure, or inappropriate use of
8 electronically stored information.

9 (b) The department by rule shall establish standards for
10 performance of risk assessments by state agencies, including
11 assessments of information resources that store or transmit
12 sensitive or critical information, and development of
13 vulnerability reports to be used in complying with rules adopted
14 under Subsection (a).

15 (c) The department by rule shall establish standards for the
16 implementation by state agencies of physical security and disaster
17 recovery requirements for computer systems that maintain sensitive
18 or critical information. The executive director may establish
19 alternate standards or exceptions to the standards adopted under
20 this subsection for certain classes of servers or mainframes.

21 Sec. 2054.065. VULNERABILITY ASSESSMENTS. (a) The
22 department shall annually rank state agencies in order of priority
23 for vulnerability assessments based on a review of agency risks,
24 the need for updated agency information, and the availability of
25 resources. Each agency identified as a priority by the department
26 shall be notified and shall use the external network vulnerability
27 assessment security services provided through the department.

1 (b) The department shall annually conduct a statewide
2 assessment of information technology security resources and
3 practices of state agencies, including an analysis of vulnerability
4 reports provided to the department under Section 2054.077. Not
5 later than December 31 of each year, the department shall submit a
6 report on the results of the department's assessment to the
7 governor, the lieutenant governor, the speaker of the house of
8 representatives, and the state auditor's office. The assessment
9 and report prepared under this section are confidential.

10 (c) In addition to other protections that may be available
11 under law, a vulnerability report and supporting documentation
12 provided to the state auditor's office under Subsection (b) is
13 incorporated into the risk assessment process of the state auditor.
14 A vulnerability report provided to the state auditor under
15 Subsection (b) is exempt from disclosure under Section 552.116.

16 SECTION 5. Subsections (b), (d), and (e), Section 2054.077,
17 Government Code, are amended to read as follows:

18 (b) In addition to any assessment required under Section
19 2054.065, the [The] information resources manager of a state agency
20 may prepare or have prepared a report, including an executive
21 summary of the findings of the report, assessing the extent to which
22 a computer, a computer program, a computer network, a computer
23 system, an interface to a computer system, computer software, or
24 data processing of the agency or of a contractor of the agency is
25 vulnerable to unauthorized access or harm, including the extent to
26 which the agency's or contractor's electronically stored
27 information containing sensitive or critical information is

1 vulnerable to alteration, damage, [~~or~~] erasure, or inappropriate
2 use.

3 (d) The [~~On request, the~~] information resources manager
4 shall provide an electronic [~~a~~] copy of the vulnerability report on
5 its completion to:

- 6 (1) the department;
7 (2) the state auditor; [~~and~~]
8 (3) the agency's executive director; and
9 (4) any other information technology security
10 oversight group specifically authorized by the legislature to
11 receive the report.

12 (e) Separate from the executive summary described by
13 Subsection (b), a [~~A~~] state agency whose information resources
14 manager has prepared or has had prepared a vulnerability report
15 shall prepare a summary of the report that does not contain any
16 information the release of which might compromise the security of
17 the state agency's or state agency contractor's computers, computer
18 programs, computer networks, computer systems, computer software,
19 data processing, or electronically stored information. The summary
20 is available to the public on request.

21 SECTION 6. Subchapter F, Chapter 2054, Government Code, is
22 amended by adding Section 2054.114 to read as follows:

23 Sec. 2054.114. COMPUTER INCIDENTS. (a) In this section, a
24 "computer incident" means a violation or imminent threat of
25 violation of computer security policies, acceptable use policies,
26 or standard computer security practices that occurs within state
27 government.

1 (b) A state agency shall promptly investigate, document,
2 and report to the department each suspected or confirmed computer
3 incident that:

4 (1) involves sensitive, confidential, or personally
5 identifiable information;

6 (2) is critical in nature; or

7 (3) could be propagated to other state systems.

8 (c) If criminal activity is suspected regarding a computer
9 incident, the state agency shall contact the department and
10 appropriate law enforcement and investigative authorities
11 immediately.

12 SECTION 7. Section 2059.001, Government Code, is amended by
13 adding Subdivision (1-a) to read as follows:

14 (1-a) "Consolidated state network" means the
15 consolidated telecommunications system defined by Section
16 2170.001.

17 SECTION 8. The Department of Information Resources shall
18 adopt rules required by Section 2054.064, Government Code, as added
19 by this Act, not later than January 1, 2008.

20 SECTION 9. This Act takes effect September 1, 2007.